ISSN : 2356 – 5195
Online ISSN: 2654 - 8704

ASESMEN KERENTANAN KEAMANAN INFORMASI SISTEM SCADA DENGAN METODE OCTAVE ALLEGRO

Chaidir Kurnia Thoullah[1], Itqan Tasyriqan*[2]
[1]Program Studi Teknik Informatika Universitas Raharja, [2]Program Studi MTI Universitas Raharja
e-mail: [1]chaidir.soedaryono@raharja.info, *[2]**itqan.tasyriqan@raharja.info**

ABSTRAK

System SCADA (Supervisory Control And Data Acquisition) merupakan sebuah system yang dibuat untuk pengambilan data, menyimpannya, analisa dan juga untuk mengendalikan suatu plant/system yang umumnya dilakukan secara jarak jauh. Untuk meningkatkan efisiensi, saat ini, system SCADA telah dipakai secara luas dalam berbagai bidang industry, seperti manufaktur, pembangkit listrik, oil & gas, telekomunikasi dan transportasi. Dalam perkembangannya, system ini tidak hanya terkoneksi secara intern saja, bahkan terkoneksi dengan internet untuk komunikasi antar komponennya maupun pengambilan informasi data sebagai bagian dari pendukung keputusan. Dengan terkoneksinya dengan system ekstern dalam hal ini internet, maka keamanan informasi system SCADA ini akan menjadi sangat rentan. Oleh karena itu, identifikasi terhadap resiko keamanan yang mungkin saja terjadi untuk memperoleh gambaran yang lengkap status keamanan system ini menjadi sangat diperlukan. Paper ini pengaplikasikan metode operationally critical threat, asset and vulnerability evaluation (OCTAVE) allegro untuk meng-asses resiko keamanan dari system SCADA. Metode ini focus pada asset informasi dan membandingkan wadah informasi yang berbeda-beda seperti database, kertas fisik dan manusia. Tujuan studi ini adalah untuk menyoroti berbagai kerentanan, resiko serta mengusulkan pendekatan mitigasi resiko yang teridentifikasi dari keamanan system SCADA. Penelitian ini diharapkan bisa digunakan sebagai dasar untuk meningkatkan keamanan system SCADA.

Kata Kunci *— SCADA, OCTAVE Allegro, Informasi, Resiko Keamanan.*

ABSTRACT

SCADA (Supervisory Control And Data Acquisition) system is a system created for data retrieval, storing, analysis and also to control a plant / system that is generally done remotely. To improve efficiency, SCADA systems are now widely used in many industries, such as manufacturing, power generation, oil & gas, telecommunications and transportation. In its development, this system is not only connected internally, even connected to the Internet for communication between its components and interchange information data as part of decision support. By connecting to the external system in this case the internet, then the information security SCADA system will be very vulnerable. Therefore, identification of possible security risks to obtain a complete picture of the security status of this system becomes indispensable. This paper applies methods of operationally critical threat, asset and vulnerability evaluation (OCTAVE) allegro to assess security risks from the SCADA system. This method focuses on information assets and compares different information containers such as databases, physical papers and human. The purpose of this study is to highlight the various vulnerabilities, risks and propose a risk mitigation approach identified from the SCADA system security. This research is expected to be used as a basis to improve the security of SCADA system.

Keyword *—SCADA, OCTAVE Allegro, Information, Security Risks.*

1. PENDAHULUAN

SCADA (Supervisory Control And Data Acquisition) merupakan system yang sangat popular yang mampu meningkatkan efisiensi dalam monitoring dan kendali peralatan-peralatan yang terdistribusi pada jarak yang jauh. System ini memainkan peranan yang sangat penting dalam otomasi dan kendali industry. System SCADA berkontribusi pada beberapa proses yang meliputi industry produksi, pengilangan, penyaringan, fabrikasi dan kelistrikan atau pembangkit listrik dalam industry-

industri seperti otomotif; heating, ventilating, and air conditioner (HVAC); heat recovery (HR) ventilation/energy recovery ventilators (EVRs); oil and gas; pengolahan air; transportasi; pembangkit, transmisi dan distribusi listrik. Saat ini system SCADA meliputi aplikasi perangkat lunak level operator untuk melihat, mengawasi dan untuk mengatasi masalah pada mesin local dan aktifitas proses. Selain operator system ini juga bias menampilkan data-data terkait produksi pada level manajemen.

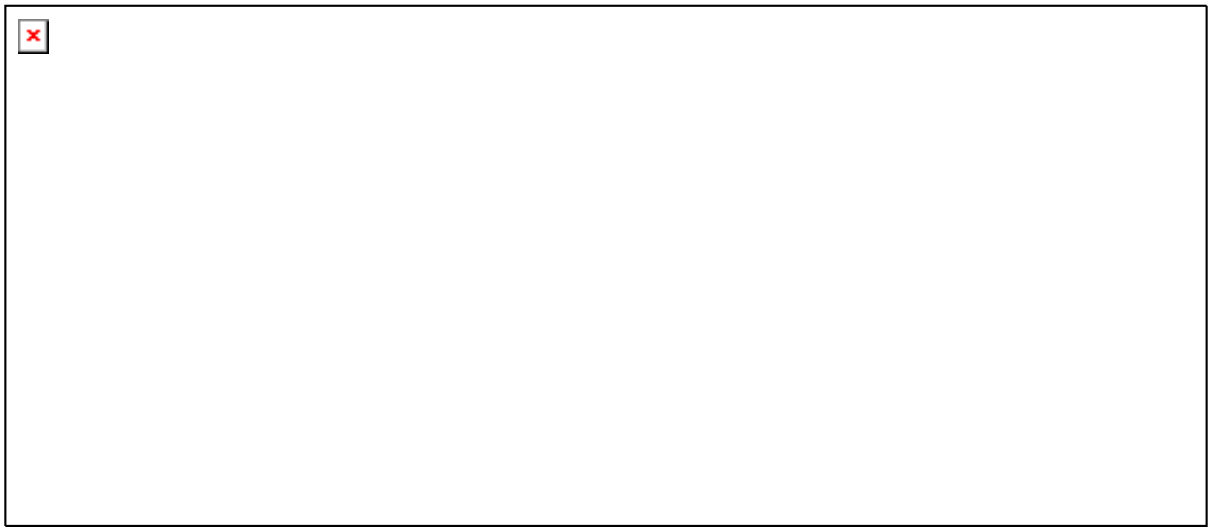
Seiring dengan berkembangnya konektifitas melalui internet, system SCADA juga mengikutinya, yang dahulu pembacaan data-data informasi terkait system hanya sampai area dimana suatu plant/pabrik berada, saat ini informasi tersebut harus bisa diakses darimana saja kapan saja sesuai dengan mobilitas para usernya. Hal ini memudahkan para user baik level enginer maupun manajemen untuk bisa mengakses informasi data secara uptodate baik untuk melakukan troubleshooting peralatan maupun dalam membuat keputusan tentang produksi. Akan tetapi disisi yang yang lain, dengan bersambungnya dengan jaringan internet, maka kerentanan pada aspek keamanan tentunya akan semakin meningkat. Hal tersebut tentunya akan menjadi masalah tersendiri yang harus diatasi. Untuk mengatasinya diperlukan asesmen yang menyeluruh tentang apa saja yang mempengaruhi keamanan suatu informasi, dimana saja titik rentannya, efek terhadap perusahaan apa dan bagaimana solusinya.

Artikel ini berusaha menjawab berusaha menjawab masalah resiko keamanan dari system SCADA. Penelitian ini diharapkan berkontribusi dalam tiga hal: pertama, riset ini mengaplikasikan metode operationally critical threat, asset, and vulnerability evaluation (OCTAVE) yang sering disebut sebagai metode asesmen resiko OCTAVE allegro untuk mengidentifikasi resiko keamanan system SCADA baik yang berasal dari dalam maupun dari luar. Kedua, penelitian akan memberikan pandangan yang bersifat holistic tentang resiko keamanan baik secara cyber maupun fisik pada domain system SCADA. Ketiga, studi ini mengajukan beberapa cara penanggulangan dari resiko yang telah teridentifikasi. Penelitian ini diharapkan berkontribusi dalam meningkatkan kebijakan keamanan system SCADA yang telah ada.

2. LANDASAN TEORI

2.1 Supervisor Control And Data Acquisition (SCADA)

SCADA merupakan kombinasi dari telemetri dan akuisisi data. SCADA melakukan proses pengumpulan informasi melalui sebuah RTU (Remote Terminal Unit), mentransfer kembali ke situs pusat, melakukan analisa dan pengendalian yang dibutuhkan kemudian menampilkannya pada beberapa layar operator. Tindakan pengendalian yang dibutuhkan kemudian diberikan ke proses yang sedang berjalan [1]. Secara ringkas SCADA merupakan kombinasi perangkat keras dan lunak computer yang dipakai untuk mengirim perintah dan menerima data yang bertujuan untuk monitoring dan pengendalian [2]. Hal tersebut tergambarkan pada Gambar 1.



Gambar 1. Contoh Layout SCADA Secara Umum [2]

Adapun manfaat dari system SCADA [1] adalah
1. Computer dapat merekam dan menyimpan data dalam jumlah yang sangat besar
2. Data dapat ditampilkan kapanpun user membutuhkannya
3. Ribuan sensor pada area yang luas dapat dikoneksikan ke system
4. Operator dapat melakukan simulasi data real ke dalam system
5. Banyak tipe data yang dapat dikumpulkan dari RTU
6. Data dapat dilihat dari mana saja, tidak hanya di site

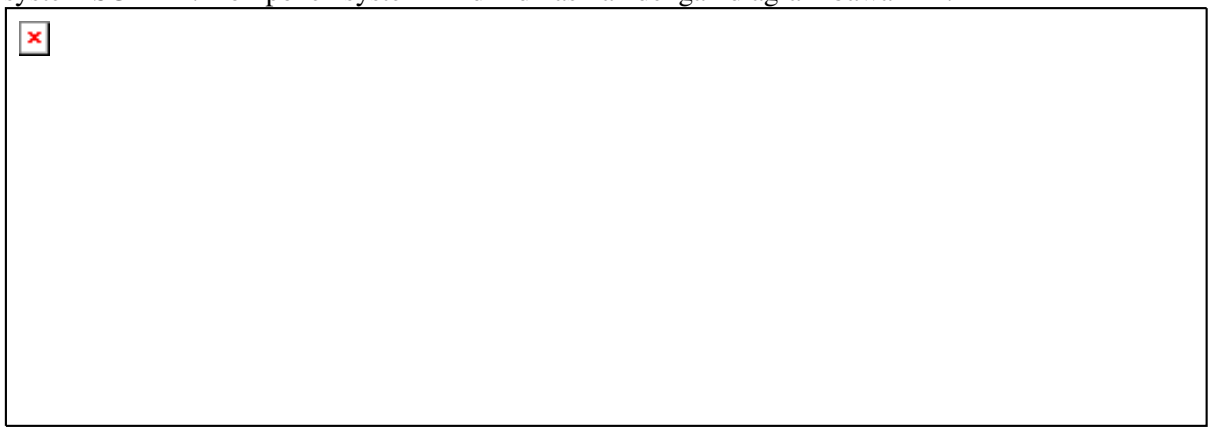
Adapun kekurangan dari system SCADA [1] adalah
1. Sistem lebih rumit daripada tipe sensor-panel
2. Kemampuan operasi yang berbeda dibutuhkan, seperti system analis dan programmer
3. Dengan ribuan sensor yang ada dibutuhkan banyak koneksi kabel
4. Operator hanya dapat melihat sejauh PLC

Dengan pertumbuhan kebutuhan akan system yang lebih kecil dan cerdas, saat ini sensor didesain dengan kecerdasan PLC dan DCS. Alat ini disebut sebagai IEDs (*Intelligent Electronic Devices*). IEDs dikoneksikkan pada fieldbus seperti Profibus, DeviceNet atau Foundation Fieldbus ke PC. Alat tersebut mempunyai kecerdasan yang cukup untuk mengambil data, berkomunikasi dengan peralatan lain serta menyimpan bagian dari keseluruhan programnya. Masing-masing dari sensor cerdas ini mempinyai lebih dari satu sensor dalam satu modul. Umumnya IED dapat mengkombinasikan input sensor analog, output analog, kendali PID, system komunikasi dan memori program dalam satu alat.

Sistem SCADA terdiri dari perangkat keras dan perangkat lunak. Perangkat keras system ini secara esensial terdiri dari lima level atau hierarki:
1. Field level instrumentation dan control devices
2. Terminal marshalling dan RTU
3. Sistem Komunikasi
4. Master Station
5. Teknologi Informasi (TI) komersial atau pemrosesan data departemen system computer.

RTU memberikan antarmuka ke sensor digital dan analog pada masing-masing sensor jarak jauh. System komunikasi memberikan jalan untuk berkomunikasi antara master station dengan site jarak jauh. System komunikasi dapat berupa kabel, fiber optic, radio, jalur telepon, gelombang mikro dan satelit. Protokol dan filosofi deteksi kesalahan dipakai untuk transfer data yang efisien dan optimal.

Perangkat lunak SCADA dapat dibagi menjadi dua tipe lisensi perusahaan dan terbuka. Perusahaan mengembangkan perangkat lunak lisensi perusahaan untuk berkomunikasi dengan perangkat keras mereka sendiri. System ini dijual sebagai solusi menyeluruh. Masalah utama dengan system ini adalah ketergantungan dengan penyedia system. Perangkat lunak terbuka sangat popular karena kemampuan untuk mencampur alat-alat yang berbeda dari berbagai perusahaan pada system yang sama yang mereka tawarkan. Sebagai contoh yang beredar di pasaran system SCADA adalah Citect dan WonderWare. Beberapa paket sekarang meliputi manajemen asset yang terintegrasi dengan system SCADA. Komponen system ini diindikasikan dengan diagram bawah ini.



Gambar 2. Diagram Komponen SCADA Secara Umum [3]

2.2 Metode OCTAVE Allegro

Metode asesmen OCTAVE Allegro pertama kali diperkenalkan oleh Caralli dkk. dan dipublikasikan oleh SEI Universitas Carnegie Mellon. Dokumen ini memberikan paparan tentang metode tersebut, instruksi terperinci bagaimana melakukan asesmen resiko OCTAVE Allegro dan standarisasi kerangka kerja yang lengkap selama proses asesmen resiko [4]. Pendekatan ini berbeda dengan pendekatan OCTAVE yang lama dengan fokus utama terhadap asset informasi dalam konteks bagaimana informasi tersebut dipakai, dimana mereka disimpan, ditransportasikan, diproses dan bagaimana mengekspos ancaman, kerentanan dan gangguan sebagai hasil. Metode ini juga sangat cocok untuk dipakai secara individual untuk menampilkan asesmen resiko tanpa keterlibatan organisasi yang luas, keahlian dan masukan [5]. Pendekatan OCTAVE Allegro terdiri dari delapan langkah yang dikelompokkan menjadi empat fase, seperti diilustrasikan pada Gambar 3.

Gambar 3. Flow Chart Metode OCTAVE Allegro [5]

Pada fase pertama (Establish Drivers), organisasi mengembangkan criteria pengukuran resiko yang konsisten sesuai dengan tujuan perusahaan. Selama fase yang kedua (Profile Assets), asset informasi yang telah ditentukan sebagai hal kritis dideskripsikan. Proses pendeskripsian ini bertujuan untuk membangun batasan yang jelas untuk asset, mengidentifikasi kebutuhan keamanannya, dan mengidentifikasi semua lokasi dimana asset disimpan, ditransportasikan atau diproses. Di fase 3 (Identify Threats), ancaman terhadap asset informasi diidentifikasi dalam konteks lokasi dimana asset tersebut disimpan, ditransportasikan atau diproses. Pada fase terakhir (Identify And Mitigate Risks), resiko terhadap asset informasi diidentifikasi dan dianalisa serta dikembangkan serta mulai mengembangkan pendekatan mitigasi.

3. METODOLOGI PENELITIAN

Penelitian ini dimulai dengan melakukan pengumpulan data yang berkaitan dengan tema yang akan dipilih. Data tersebut dikumpulkan dengan studi literature maupun dengan melakukan pengamatan secara langsung/observasi. Studi literature dilakukan dengan mencari artikel terkait baik dalam bentuk buku ataupun jurnal ilmiah. Sedangkan observasi dilakukan di sebuah perusahan distribusi listrik yang telah menggunakan system SCADA.

Setelah data terkumpul, kemudian data tersebut dianalisa dengan menggunakan metode OCTAVE allegro. Metode ini akan menganalisa kerentanan asset informasi yang berkaitan dengan system SCADA, melakukan profiling asset, mengidentifikasi ancaman dan mengidentifikasi serta mitigasi terhadap resiko. Hasil akhirnya berupa laporan yang dapat digunakan sebagaai bahan pertimbangan untuk meningkatkan keamanan informasi, yang dalam hal ini adalah informasi system SCADA.

4. LITERATUR REVIEW

Dalam penelitian ini dilakukan studi literatur terhadap beberapa jurnal ilmiah yang bertemakan sistem SCADA. Mihai Jacob dkk. [6] Memaparkan tentang teori dan praktek sisten SCADA dalam skala laboratorium dalam artikelnya yang berjudul Supervisory And Data Acquisition Laboratory. Agape C.P [7] dkk.melakukan penelitian dengan mensimulasikan sistem SCADA menggunakan papan pengembangan Tiny Tiger 2 yang digunakan untuk akuisisi dan kendali sistem distribusi listrik tegangan menengah. Alexandru Ujierosi [8] menjelaskan tentang evolusi sistem SCADA dalam perkembangannya selama lebih dari 50 tahun dalam hal arsitektur dan sistem utamanya. Dalam artikelnya Amir Shahzad dkk. [9] Membahas tentang pengukuran keamanan sistem SCADA yang berhubungan dengan pemrosesan dengan sesi khusus dari polling otomatis, analisa mekanisme kriptografi dan memberikan solusi keamanan inklusif dalam distributed network protocol version 3 (DNP3) sebagai bagian dari sistem SCADA. Dalam artikelnya yang lain Amir Shahzad dkk. [10] Melakukan penelitian dengan desain simulasi sistem pompa air dimana beberapa titik jaringan ada yang dihubungkan dengan kabel maupun nirkabel terhadap sensor-sensor yang dimonitor dengan pengendali utama sebagai bagian dari sistem SCADA. Untuk alasan keamanan dan tujuan verifikasi byte data, sebuah mekanisme dibutuhkan untuk diberlakukan pada pseudo-transport layer dengan menggunakan algoritma kriptografi.

Jose M. Moya dkk. [11] Mengajukan sebuah sistem yang dikembangkan dengan agen terdistribusi berbasis algoritma unsupervised learning (self-organizing maps) untuk mencapai toleransi terhadap kesalahan data dan meningatkan ketahanan terhadap serangan-serangan yang tidak diketahui sebelumnya. Radoje CVEJIC dkk. [12] Dalam artikelnya melakukan penelitian dengan mengimplementasikan sistem SCADA dalam plant tegangan tinggi di pembangkit listrik Kostolac. Wenyu Zhao dkk. [13] Melakukan peneltian dan pengembangan menggunakan data yang diambil dari sistem SCADA dan CMS untuk melakukan prediksi tentang kondisi turbin offshore 3 MW. Dehua Zheng dkk. [14] Menggunaan data SCADA untuk melakukan peramalan terhadap kekuatan angin pada pembangkit listrik tenaga angin yang akhirnya diketahui trending daya yang akan dibangkitkan dalam sehari kedepan. Wenna Zhang dkk. [15] Meneliti tentang penggunaan data sistem SCADA yang diolah dengan metode K-Means untuk memonitor kondisi pembangkit listrik tenaga angin.
Marius Sokolewicz dkk. [16] Menggunakan sistem SCADA sebagai pengendali otomatis dan untuk memonitor air yang masuk dari sungai Magdalena, Colombia yang tujuan akhirnya adalah asesmen terhadap resiko banjir. Aumar Al-Nakeeb dkk. [17] Dalam penelitiannya membahas tentang pemakaian sistem SCADA untuk mengoperasikan , mengelola proses dan diagram instrumentasi pada plant pengolahan air di Sharq Dilja, Bagdad Irak. Ahmad Budi Setiawan [18] merekomendasikan strategi desain pada pengembangan keamanan smart grid cyber pada siste SCADA. Ibrahim Anafi dkk. [19] Mengusulkan implementasi sistem SCADA berbiaya murah menggunakan modul arduino uno. Cosmin Ursomu dkk. [20] Menerangkan tentang sistem SCADA yang dipakai pada pembangkit listrik dalam hal pengawasan dan pengendalian sistem oleh operator. Agus Eko Handoko dkk. [21] Membuat rancang bangun sistem SCADA untuk memperoleh data pada saat waktu tertentu untuk menentukan kebutuhan PAC pada operasional instalasi pengolahan air. Abdal Hossein Rezai dkk. [22] Melakukan review pada skema kunci manajemen yang ada pada jaringan SCADA yang mana akan memberikan arahan untuk penelitian-penelitian selanjutnya pada bidang ini.
Dari literatur yang ada dapat disimpulkan bahwa tema yang dibahas adalah tentang implementasi sistem SCADA,penggunaan dan pengolahan data SCADA dan keamanan sistem SCADA. Tema keamanan ini baru sedikit dibahas sehingga penulis memilih tema ini untuk penelitian.

5. HASIL DAN ANALISA

Tujuan dari bagian ini yang pertama adalah mengumpulkan semua ancaman keamanan yang didapatkan dengan melakukan asesmen resiko keamanan informasi dengan menggunakan metode OCTAVE Allegro. Hasil dari penelitian ini ditampilkan pada table 1 dan 2, yang mana member pandangan yang lebih baik dari ancaman keamanan yang teridentifikasi dan resiko potensial dari sebuah system SCADA. Table tersebut memperlihatkan asset informasi yang diidentifikasi dan

dipakai dalam proses asesmen resiko, ancaman yang terkait dan konsekuensi atau dampak potensial dalam bentuk resiko spesifik dan skornya.

Tabel 1 memperlihatkan identifikasi ancaman sebagai hasil studi dari system SCADA dalam sudut pandang cyber dan fisik dan berdasarkan container asset yang berbeda-beda. Resiko yang teridentifikasi meliputi otentifikasi dan kebiasaan user, peralatan system SCADA serta pertukaran data diantara alat-alat yang ada melalui internet. Di table 2, dampak yang mungkin atau resiko potensial yang ditentukan dan dihubungkan ke asset dan ancaman yang disebutkan dalam table 1. Dalam peniruan legitimasi user system SCADA di table 1 (ID ancaman 1), seseorang berusaha untuk meniru dan bertindak seolah sebagai user yang asli. Untuk mencapai tujuan itu, dibutuhkan akses pada informasi rahasia user yang biasanya berupa ID user dan password. Akses terhadap informasi itu dapat dilakukan dengan social engineering atau mengintersep data yang digunakan untuk mengakses sitem SCADA. Social engineering merupakan sebuah pendekatan untuk menipu atau mempengaruhi orang untuk membuka informasi yang sensitive. Program yang berbahaya dapat diinjeksikan pada aplikasi yang diinstal pada system SCADA, yang mana bisa memungkinkan penyerang untuk mengeksekusi operasi yang membahayakan. Ancaman injeksi kode berbahaya dapat juga bertujuan untuk mencuri informasi rahasia tentang user (ID 1).

Table 1. Ancaman keamanan yang didapatkan dengan melakukan asesmen resiko informasi

ID Aset	Aset Informasi	Kemungkinan Ancaman Keamanan
1	Kerahasiaan user	Peniruan user Pencurian identitas dan informasi rahasia
2	Informasi yang dikumpulkan alat Status informasi SCADA	Modifikasi informasi Serangan denial-of-service (DoS) Pengambil alihan alat atau sensor Pembukaan informasi Interupsi fungsi
3	Struktur SCADA Informasi inventori	memperoleh akses ke informasi inventori untuk mencari peralatan khusus yang rentan untuk menyerang system SCADA
4	Informasi log	memperoleh akses untuk data log dan memperoleh informasi yang berguna agar bisa memungkinkan serangan terhadap system SCADA
5	Informasi yang ditransmisikan lewat gateway	Mencuri informasi dari paket yang ditransmisikan lewat gateway
6	Informasi setup SCADA	Modifikasi informasi
7	Sumber informasi (dokumen, database)	Mencuri informasi pribadi Membuat media tidak dapat diakses sehingga terjadi kegagalan hardware

Table 2. Resiko yang teridentifikasi dengan asesmen resiko informasi dalam hal dampak dan skor resiko

ID Ancaman	Dampak Yang Mungkin (Resiko)	Skor Resiko
1	Akses tidak terotorisasi terhadap system SCADA Eksekusi tidak terotorisasi terhadap system SCADA Kehilangan kendali terhdap system SCADA	41
2	Pengukuran sensor dimanipulasi untuk menyusup pada system SCADA Kerugian financial	39
3	Penyerang mengidentifikasi peralatan paling rentan Penyerang mengambil alih kendali system SCADA Kerugian financial	39
4	Penyerang mendapatkan cara untuk mengakses system utama Penyerang mengganti konfigurasi system dan menambahkan	39

	program berbahaya Kerugian financial	
5	Kemungkinan bisa membuat system down atau membuatnya tidak berguna sama sekali Kemungkinan untuk injeksi kerentanan keamanan yang baru ke dalam system	39
6	Kesulitan dalam mensetting system SCADA Kemungkinan malfungsi system SCADA Kerugian financial	36
7	Kehilangan system informasi	23

Ancaman pengambilalihan peralatan di table 1 (ID 2) akan menyebabkan sensor tidak dapat mendeteksi resiko fisik, seperti kebakaran, banjir atau pergerangan yang aneh di plant. Disamping itu, dengan pencurian informasi dari sensor yang terpasang (ID ancaman 5), seorang penyerang dapat menginjeksikan kode berbahaya, virus atau worm dalam lalu lintas data dan melepaskannya di system. Secara intensif pemakaian sumberdaya system melalui self-replication akan mengakibatkan system tidak dapat menyelesaikan pekerjaan yang relevan dan akan membuat system down sehingga pada periode waktu tertentu system SCADA benar-benar menjadi tidak berfungsi. Selanjutnya untuk keterangan lebih terperinci dan contoh kasus pada dunia nyata yang berhubungan dengan kemungkinan resiko yang telah disebutkan pada table 2 dapat dilihat pada table 3.

Table 3. Contoh kasus di dunia nyata yang terkait dengan identifikasi ancaman keamanan dan resiko dari asset-aset informasi yang berbeda.

ID Aset	Contoh Dalam Dunia Nyata
1	Seseorang yang tidak otoritas memperoleh informasi rahasia dan bisa login ke system SCADA.
2	Seseorang mengubah data pembacaan dari smart-meter sehingga pemakaian listrik seolah-olah lebih tinggi atau rendah. Mengubah status on/off peralatan sehingga akan membuat bingung operator. Melakukan modifikasi pada layer fisik sensor sehingga sensor tidak bisa mendeteksi resiko seperti kebakaran, banjir dan lain-lain.
3	Penyerang dapat mengakses asset informasi dengan mengambil media back-up yang tidak terenkripsi atau melalui social-engineering.
4	Asset ini dapat diperoleh apabila log data dengan mudah bisa diakses melalui jalur yang tidak aman.
5	Asset ini dapat diperoleh apabila gateway tidak sepenuhnya aman seperti jaringan wifi terbuka. Penyusup dapat membajak wifi dapat menginjeksi dengan kode berbahaya dan mengambil kendali system SCADA secara keseluruhan.
6	Aset ini dapat diperoleh bila asset informasi disimpan dalam system SCADA tanpa mekanisme autentifikasi yang kuat.
7	Asset ini dapat diperoleh secara fisik atau digital, seperti pada kertas, CD, DVD, media backup, jaringan komunikasi maupun database. Informasi dapat diakses oleh orang yang tidak terotorisasi bila tidak disimpan dengan aman dan benar.

Penanganan yang mungkin untuk melindungi asset informasi dan membuat system SCADA menjadi lebih aman, tertera pada table 4. Kunci dari pendekatan mitigasi yang diajukan adalah konfigurasi teknis yang benar, autentifikasi user yang kuat dan kesadaran semua user system SCADA. Penanganan yang diajukan berkorelasi dengan ancaman dan resiko keamanan. Pemakaian metode autentifikasi yang kuat seperti identifikasi biometric (finger print, bentuk geometri tangan, scan retina, pola tubuh dan tandatangan) merupakan pencegahan pertama yang diusulkan pada table 4. (ID ancaman 1). System biometric ini juga baik untuk dimplementasikan pada platform perangkat keras. Akan tetapi cara terbaik pada masalah autentifikasi ini adalah memberikan kesadaran pada user secara berkelanjutan dan program pendidikan. Autentifikasi multi-faktor adalah proses autentifikasi menggunakan dua atau lebih data yang diberikan oleh user.

Table 4. Proposed security threat and risk countermeasures to be applied in IoT-based smart home environments.

ID Ancaman	Pendekatan Mitigasi Yang Mungkin
1	Akses ke system dengan menggunakan pengenal biometric. Mengimplementasikan program kesadaran kepada user sehingga menyadari akan social-engineering. Mengimplementasikan autentifikasi multi-factor
2	Menggunakan jalur komunikasi dengan pemakaian VPN yang aman. Membatasi lalulintas jaringan sehingga hanya dapat diakses oleh user yang terotorisasi. Mengembangkan program pelatihan kesadaran keamanan untuk user system SCADA.
3	Memakai intrusion detection system (IDS)/intrusion prevention system (IPS). Memakai enkripsi untuk transmisi data. Melakukan backup data untuk menjaga data-data penting.
4	Mengamankan lokasi dimana peralatan dipasang. Memberikan akses yang aman ke interface yang digunakan untuk mengkonfigurasi alat. Mengubah password default pada peralatan yang dipasang.
5	Menggunakan perangkat lunak dan keras untuk menguji lalulintas jaringan. Membuat backup konfigurasi system kerja. Selalu memonitor kinerja system.
6	Mengaplikasikan mekanismen autentifikasi yang kuat. Memberikan program kesadaran dan pelatihan tentan keamanan system. Memastikan konfigurasi system aman dan dilakukan oleh orang yang berhak.
7	Menggunakan hanya jaringan yang terpercaya. Membagi informasi secara hati-hati dan terbatas. Memakai hanya provider terpercaya untuk menerima support teknis untuk kegagalan perangkat keran system SCADA.

Pada table 4 (ID ancaman 30, dengan memakai jalur komunikasi yang aman, membatasi akses trafik hanya untuk user yang berhak dan memberikan pelatihan keamanan, modifikasi, tebukanya dan pengambilalihan sensor atau peralatan dapat dihindari. Hal ini seharusnya akan mengakibatkan berkurangnya potensi resiko pada manipulasi peralatan dan oleh karena itu akan mengurangi kerugian financial. Scenario ini dapat juga diaplikasikan pada ID ancaman 6.

Pengujian trafik jaringan secara periodic, mengamankan akses untuk konfigurasi system dan memonitor kinerja system akan menjaga dari pencurian informasi data melalui jaringan SCADA. Hal ini akan mengurangi downtime system, kemungkinan membuang sumber daya system, dan mencegah kerentanan keamanan yang baru diinjeksikan ke dalam system. Melakukan backup dan pengarsipan data, (ID ancaman 4), menjaga salinan data sensistif akan dapat melindungi dari kerusakan data baik secara fisik maupun teknis. Pengamanan media backup harus diyakinkan dengan menerapkan kebijakan keamanan, menetapkan akses software backup hanya pada orang yang berhak, menyimpan backup diluar site, mengendalikan akses fisik terhadap tempat dimana backup disimpan, pemakaian media backup tahan api dan aman serta dienkripsi dan di-password.

Pengamanan lokasi fisik dan akses terhadap interface konfigurasi alat harus dengan menggunakan akun. Pendekatan mitigasi yang diusulkan, (ID ancaman nomor 5), memperlihatkan masalah ini dan merekomendasikan pertimbangan keamanan secara fisik. Apabilan autentifikasi biometric diintegrasikan dengan system SCADA, pendekatan yang sama dapat diterapkan pada ancaman logical dan fisik. Dengan menerapan hal tersebut, akan meningkatkan efektifitas biaya system SCADA. Penting disebutkan bahwa pendekatan mitigasi yang telah diberikan tidak memberikan solusi penuh terhadap ancaman dan resiko yang teridentifikasi, akan tetapi hal ini akan membatasi ancaman dan mengurangi resiko dan konsekuensi keamanan. Pemilihan provider terpercaya untuk internet dan komponen system merupakan bagian dari pendekatan mitigasi, disebutkan pada table 4 (ID ancaman

7). Selanjutnya, untuk menjaga system agar beroperasi berkelanutan, perawatan rutin, pengecekan konfigurasi dan perbaikan terhadap kekurangan system harus dilakukan oleh personel bersertifikat dan terlatih dengan baik serta berdasarkan kontrak legal.

6. KESIMPULAN

Teknologi system SCADA saat ini memberikan kemudahan sekaligus juga resiko terhadap keamanan system. Saat ini system SCADA telah terhubung dengan jaringan LAN, WAN atau bahkan internet sehingga membuat system keamanan informasinya menjadi sangat rentan baik dari serangan luar maupun dalam. Bila system atau komponen yang berada dalam system dapat ditembus, maka privasi user, data-data system atau bahan system dapat dikendalikan oleh orang yang tidak mempunyai hak. Asesmen terhadap resiko yang komprehensif sangat dibutuhkan sehingga akhirnya akan memberikan solusi yang relevan. Paper ini melakukan asesmen menggunakan metode OCTAVE allegro dan mendapatkan 7 aset cyber dan fisik yang kritis. Sebagai hasilnya ada sekitar 14 resiko keamanan yang berasal dari dalam maupun luas system SCADA yang teridentifikasi. Konsekuensi atau dampak dari resiko ini telah dijelaskan dan penanggulangan/pencegahan yang sesuai terhadap resiko juga telah dikemukakan.

DAFTAR PUSTAKA

[1] Clarke, Gordon And Deon Reyders. 2004. *Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems*. Oxford : Newness.

[2] API Standard 1164. 2009. *Pipeline SCADA Security*. Washington : API.

[3] Knapp, Eric. 2011. *Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Watham : Syngress.

[4] Keating, Corland Gordon. 2014.*Validating the OCTAVE Allegro Information Systems Risk Assessment Methodology: A Case Study*. Florida : Nova Southeastern University.

[5] Caralli, Richard A., James F. Stevens, Lisa R. Young And William R. Wilson. 2007. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Hanscom : Software Engineering Institute.

[6] Iacob, M; Bejan,CA; Andreescu,GD. *Supervisory Control and Data Acquisition Laboratory*. Telfor Journal, 2010, 2(1) :49 – 54.

[7] Rafika, A. S., Budiarto, M., & Budianto, W. (2015). Aplikasi Monitoring sistem absensi sidik jari sebagai pendukung pembayaran biaya pegawai terpusat dengan SAP. *CCIT Journal*, *8*(3), 134-146.

[8] Agape, CP; Kilyeni,ST; Barbulescu,C. *SCADA System Simulation Using The Tiny Tiger 2 Development Board.* Journal Of Sustainable Energy, December, 2015, 6(4): 180 – 183.

[9] Ujvarosi, A. *Evolution Of SCADA Systems*. Bulletin of the Transilvania University of Braşov, 2016, 9(58) : 63 – 68.

[10] Shahzad, A; Lee,M; Kim, HD; Woo, S; Xiong, N. *New Security Development and Trends to Secure the SCADA Sensors Automated Transmission during Critical Sessions*. Symmetry, 2015, *7:* 1945-1980; doi:10.3390/sym7041945

[11] Shahzad, A; Lee, M; Xiong, NN; Jeong, G; Lee, YK; Choi, JY; Mahesar, AW. *A Secure, Intelligent, and Smart-Sensing Approach for Industrial System Automation and Transmission over Unsecured Wireless Networks*. Sensors, 2016, 16(322):1-18; doi:10.3390/s16030322

[12] Moya, JM; Araujo, A; Bankovic, Z; Goyeneche, JM; Vallejo, JC; Malagon, P, Villanueva, D; Fraga, D; Romero, E; Blesa, *J. Improving Security for SCADA Sensor Networks with Reputation Systems and Self-Organizing Maps*. Sensors,2009 , 9 : 9380-9397; doi:10.3390/s91109380.

[13] Cvejic, R; Markovic, A; Cvejic, R. *Supervisory Control (SCADA) Systems And Their Implementation In The High Voltage Plants*. Annals Of The University Oradea Fascicle 1 of Management and Technological Engineering, December 2014, 3 : 165 – 169.

[14] Zhao, W; Siegel, D; Lee, J; Su, L. *An Integrated Framework of Drivetrain Degradation Assessment and Fault Localization for Offshore Wind Turbines*. International Journal of Prognostics and Health Management, 2013, 012 : 1 – 13; ISSN 2153-2648.

[15] Zheng, D; Shi, M; Wang, Y; Eseye, AT; Zhang, J. *Day-Ahead Wind Power Forecasting Using a Two-Stage Hybrid Modeling Approach Based on SCADA and Meteorological Information, and Evaluating the Impact of Input-Data Dependency on Forecasting Accuracy*.Energies, 2017, 10(1988) : 1 24; doi:10.3390/en10121988

[16] Zhang,W; Ma, X. *Simultaneous Fault Detection and Sensor Selection for Condition Monitoring ofWind Turbines*. Energies, 2016, 9(280) : 1 – 12; doi:10.3390/en9040280

[17] Sokolewicz, M; Wijma, E; Nomden, H; Driessen, T; Agten, QV; Carnajal, F. *Flood protection as a key-component of the environmental restoration of Canal del Dique, Colombia*. 3rd European Conference on Flood Risk Management : FLOOD*risk, 2016;* DOI: 10.1051/e3sconf/2016

[18] Al-Nakeeb, A; Al-Samawi,AA ; Al-Saffar, HA. *Upgrading of Alum Preparation and Dosing Unit for Sharq Dijla Water Treatment Plant by Using Programmable Logic Controller System*. Journal Of Engineering, February 2018, 24(2) : 131 – 141.

[19] Setiawan, AB. *Peningkatan Keamanan Supervisory Control And Data Acquisition (SCADA) Pada Smart Grid Sebagai Infrastruktur Kritis*. JPPI, 2016, 6(1) : 59 – 78; DOI: 10.17933/jppi.2016.060104

[20] Allafi, I; Iqbal, T. *Low-Cost SCADA System Using Arduino and Reliance SCADA for a Stand-Alone Photovoltaic System*. Journal of Solar Energy, 2018, 2018 : 1 – 8; https://doi.org/10.1155/2018/3140309

[21] Ursoniu, C; Pepa, D.*Scada Systems – Control, Supervision and Data Acquisition for the Power Plants Settled on a Stream (Part 1)*. ANALELE UNIVERSITĂȚII "EFTIMIE MURGU" REŞIȚA, 2015, 22(2) : 378 – 389; ISSN 1453 – 7397

[22] Handoko, AE; Erizal; Chadirin, Y. Rancang Bangun Sistem Scada (*Supervisory Control And Data Acquisition*) pada Instalasi Pengolahan Air Sungai Cihideung Institut Pertanian Bogor. JTEP, Oktober 2017, 5(2) : 129-136; P-ISSN 2407-0475 E-ISSN 2338-8439; DOI: 10.19028/jtep.05.2.129-136.

[23] Rezai, A; Keshavarzi, P; Moravej. *Key management issue in SCADA networks: A review*. Engineering Science and Technology, an International Journal, 2016, 20 (2017) : 354–363